

May 23, 2016

The Honorable Thomas Wheeler  
Chairman  
Federal Communications Commission  
445 12<sup>th</sup> Street, SW  
Washington, DC 20554

Dear Chairman Wheeler:

The Federal Communications Commission's (FCC) rules and regulations for the communications sector can have a significant effect on the security of individual Americans, our critical infrastructure, and our national and economic security. Given our committees' past work on cybersecurity, we have an interest in the Commission's current Notice of Proposed Rulemaking related to set-top boxes (MB Docket No. 16-42).<sup>1</sup> In particular, we are interested in learning more about the cybersecurity proposals within the rulemaking and urge further attention in this area. It is important that cybersecurity is fully addressed in any final rule.

As more and more devices become directly connected to the Internet, it is imperative that they be developed with adequate levels of security in mind. Vulnerabilities in software and hardware can allow malicious actors to infect consumers' devices and carry out cyberattacks. These attacks could allow criminals from across the globe to access networks and steal sensitive data. Further, without the right cybersecurity protections across networks, a vulnerable device could allow cybercriminals entry.

The communications sector has invested significant resources in the development and use of the NIST Cybersecurity Framework.<sup>2</sup> While the Framework itself is voluntary, many current communications providers are actively using it today to complement or support their existing security programs.<sup>3</sup> It is unclear how some of the FCC's proposed rulemaking aligns with the Framework's recommended practices or how existing cable and satellite providers can adequately inventory devices attached to their network, including devices owned by a third party. For example, a core function of the Framework is to identify a firm's information technology assets and connections with other organizations and devices in order to ensure that it fully understands its risk posture and develops an associated cybersecurity risk management program.

To better understand how the Commission's current proposed rule-making related to set-top boxes impacts cybersecurity, we respectfully request the following information:

1. How did the FCC consider cybersecurity when developing the proposed rulemaking?

---

<sup>1</sup> *Expanding Consumers' Video Navigation Choices; Commercial Availability of Navigation Devices*, Notice of Proposed Rulemaking and Memorandum Opinion and Order, 31 FCC Rcd 1544 (2016) ("NPRM").

<sup>2</sup> National Institute of Standards and Technology, Cybersecurity Framework, <http://www.nist.gov/cyberframework/>.

<sup>3</sup> *Id.*


May 23, 2016

Page 2


2. The FCC requires self-certifications related to a number of issues, how will the FCC enforce this?
3. How does the proposed rulemaking ensure that third-party device manufacturers and software developers are meeting an adequate level of software and hardware security, including supply chain risks?
4. Did the FCC consider the NIST Cybersecurity Framework risk management approach in the proposed rule-making?
  - a. If yes, please describe how and cite the references in the proposed rulemaking.
  - b. If no, can you assure us the Framework will be considered as you draft final rules?
5. Does the proposed rulemaking address potential economic harm to content creators or businesses that may be impacted from the potential for cyberattacks or potential harm to infrastructure?

Please provide this information as soon as possible, but no later than 5:00 p.m. on June 10, 2016. If you have any questions about this request, please contact Brooke Ericson of the Senate Homeland Security and Governmental Affairs Committee Majority staff at (202) 224-4751; Brett DeWitt of the House Homeland Security Committee Majority staff at (202) 226-8417; Matt Grote of the Senate Homeland Security and Governmental Affairs Committee Minority staff at (202) 224-2627; and Christopher Schepis of the House Homeland Security Minority staff at (202) 226-2616. Thank you for your prompt attention to this matter.


Sincerely,




Ron Johnson  
Chairman  
Senate Committee on Homeland Security  
& Governmental Affairs



Thomas R. Carper  
Ranking Member  
Senate Committee on Homeland Security  
& Governmental Affairs



Michael T. McCaul  
Chairman  
House Committee on Homeland Security



Bernie G. Thompson  
Ranking Member  
House Committee on Homeland Security

cc. Commissioner Clyburn  
Commissioner O'Rielly  
Commissioner Pai  
Commissioner Rosenworcel  
U.S. Department of Homeland Security Secretary Jeh Johnson





FEDERAL COMMUNICATIONS COMMISSION  
WASHINGTON

OFFICE OF  
THE CHAIRMAN

June 10, 2016

The Honorable Thomas R. Carper  
Ranking Member  
Committee on Homeland Security and Governmental Affairs  
United States Senate  
442 Hart Senate Office Building  
Washington, D.C. 20510

Dear Senator Carper:

Thank you for your recent letter inquiring how the Federal Communications Commission (FCC) is addressing cybersecurity issues as part of our current rulemaking efforts to comply with the Communications Act's mandate for consumer choice in television navigation tools.

Protecting the nation's networks is a top priority for the FCC. Commission personnel work around the clock—including in a 24/7 operations center—to safeguard America's telephone, radio, cable, satellite, and Internet connectivity. The Commission takes our security responsibilities very seriously, and we leverage extensive staff expertise to ensure our policy proposals accord with best practices and the best available science.

We bring this cybersecurity experience and awareness to all of the rulemakings we undertake to fulfill our responsibilities under the Communications Act, including our current efforts to update our rules implementing section 629 of the Act. Adopted by Congress in 1996, section 629 requires the Commission to promote competition in the market for devices that consumers use to access their pay-television content.<sup>1</sup> The Notice of Proposed Rulemaking (NPRM) we adopted earlier this year proposes updating our rules implementing section 629 to allow device manufacturers and other innovators to develop devices or software that will give pay-television subscribers new ways to access the content they have purchased.<sup>2</sup>

We took this action because consumers have few alternatives to leasing set-top boxes from their pay-television providers. The statutory mandate is not yet filled. This lack of competition has meant few choices and high prices for consumers. In a recent Rasmussen Reports study, 84 percent of consumers felt their cable bill was too high. Included in every bill is a no-option, add-on fee for set top box rental. According to a congressional study, consumers spend, on average, \$231 in rental fees annually. Even worse for consumers, these rental fees continue to increase.<sup>3</sup> And while MVPD set-top boxes are increasingly connected to the Internet,

---

<sup>1</sup> 47 U.S.C. § 629.

<sup>2</sup> Expanding Consumers' Video Navigation Choices, 81 Fed. Reg. 14033 (proposed Mar. 16, 2016).

<sup>3</sup> One recent analysis found that the cost of cable set-top boxes has risen 185 percent since 1994 while the prices of computers, televisions, and mobile phones have dropped by 90 percent during that same time period. Consumer



they have been greatly outpaced in functionality and convenience by online video devices and apps.

The NPRM proposes a careful balance between network security and section 629's mandate that consumers be able to enjoy pay-television content with the equipment of their choice. Cable and satellite providers would be required to support a narrow, defined set of interfaces that would allow competitive devices and apps to access television content. These types of interfaces, usually termed Application Programming Interfaces (APIs), are routinely offered by online services. APIs allow a third party (such as a consumer navigation device provider) to interface with an organization's systems, without revealing any internal design, operation, or data about the organization. Third parties that connect to an API are not granted full system access, and are limited to only the features provided by the API. Securing an API is easier than securing internal systems, because an API only has to support specific functionality. Best practices for API security are readily available and widely practiced.<sup>4</sup>

The proposal would bring to television services the same secure modularity that phone and Internet customers have long enjoyed. In the telephone context, for example, a user can purchase and operate a third-party (e.g. Samsung) phone; the phone is not granted full access to telephone carrier (e.g. Verizon) internal systems. Similarly, in the Internet context, a user can purchase and operate a third-party (e.g. Arris) modem; that modem is not granted full access to the Internet Service Provider's (e.g. Comcast) internal systems.

All of the major cable and satellite providers, in fact, already support APIs for authenticating user credentials—some of the most sensitive information in the television ecosystem. Services like HBO Go<sup>5</sup> and Showtime Anytime<sup>6</sup> ensure that customers have subscribed by interfacing with cable and satellite account management systems. These APIs have been supported for over 5 years.

Finally, the FCC's set-top box proposal would in no way alter the role of digital rights management (DRM) platforms in the television ecosystem. DRM platforms offer rigorous protection against unauthorized copying and other violations of content owner rights.<sup>7</sup> Under the FCC's proposal, content owners would remain free to select the DRM platforms that they prefer. Developers of competitive set-top boxes and apps would license the DRM technology and satisfy compliance requirements – in the very same way that current set-top boxes support DRM, and the same way that competitive devices and apps already support DRM for online video.

---

Fed'n Am. & Pub. Knowledge, Comment Re: Media Bureau Request for Comment on DSTAC Report, MB Docket No. 15-64 (Jan. 20, 2016).

<sup>4</sup> See, e.g., *OWASP Enterprise Security API Project*, OPEN WEB APPLICATION SOC'Y PROJECT [https://www.owasp.org/index.php/Project\\_Information:\\_OWASP\\_Enterprise\\_Security\\_API\\_Project](https://www.owasp.org/index.php/Project_Information:_OWASP_Enterprise_Security_API_Project) (last visited June 2, 2016).

<sup>5</sup> HBO GO, <http://play.hbogo.com> (last visited June 2, 2016).

<sup>6</sup> SHOWTIME ANYTIME, <http://www.showtimeanytime.com> (last visited June 2, 2016).

<sup>7</sup> See DOWNLOADABLE SEC. TECH. ADVISORY COMM., DSTAC FINAL REPORT 262-67 (Aug. 28, 2015), <https://transition.fcc.gov/dstac/dstac-report-final-08282015.pdf> [hereinafter DSTAC FINAL REPORT].



Furthermore, all of the major DRM platforms support revoking authorization for content; if a competitive device or app were ever found to be violating DRM requirements, access to content could be immediately terminated.

Please find below answers to the specific questions in your letter.

*1. How did the FCC consider cybersecurity when developing the proposed rulemaking?*

The NPRM was prompted in part by a congressional directive within the STELA Reauthorization Act of 2014.<sup>8</sup> Section 106(d) of that legislation required FCC to assemble a working group of technical experts to evaluate and recommend options for enhancing downloadable security systems designed to promote the competitive availability of navigation devices. The FCC promptly implemented Congress's directive by chartering the Downloadable Security Technology Advisory Committee (DSTAC) on December 5, 2014.

This DSTAC's membership consisted of diverse technical experts, drawn from content creators, cable and satellite providers, consumer electronics manufacturers, software vendors, public interest organizations, and academia.<sup>9</sup> The group first convened on February 23, 2015. After weekly conference calls and additional in-person meetings, the committee issued its final 344-page report on August 28, 2015.<sup>10</sup> The FCC also received over 100 comments and other submissions in association with this process.<sup>11</sup> You can find this report and other DSTAC materials at: <https://www.fcc.gov/about-fcc/advisory-committees/general/downloadable-security-technology-advisory-committee>.

The DSTAC's participants and commenters provided valuable technical guidance to the Commission, with particular emphasis on security and privacy matters. Over 100 pages of the committee's final report expressly address cable and satellite network security, protecting content, or safeguarding consumer data.<sup>12</sup> Many comments and submissions also addressed security issues.

In sum, the FCC solicited and benefited from a wealth of security expertise while developing the proposed rulemaking, and we carefully evaluated the input that we received. The Notice of Proposed Rulemaking seeks additional input from stakeholders on the security aspects of the Commission's proposal.<sup>13</sup>

---

<sup>8</sup> STELA Reauthorization Act of 2014, Pub. L. No. 113-200, § 106(d), 128 Stat. 2059 (2014)

<sup>9</sup> *Appointment of Members to the Downloadable Security Technology Advisory Committee*, 30 FCC Rcd. 389 (Jan. 27, 2015).

<sup>10</sup> DSTAC FINAL REPORT, *supra* note 9.

<sup>11</sup> See MB Docket No. 15-64.

<sup>12</sup> See DSTAC FINAL REPORT, *supra* note 9, at 3-4, 12-16, 24-26, 28-30, 31-37, 47-56, 60-135, 186-192.

<sup>13</sup> Expanding Consumers' Video Navigation Choices, *supra* note 1, ¶¶ 50-62, 70-80.



*2. The FCC requires self-certifications related to a number of issues, how will the FCC enforce this?*

The Communications Act and Commission rules guarantee a set of public interest features for current cable and satellite set-top boxes.<sup>14</sup> These features include strong security and privacy protections, Emergency Alert System messaging, closed captioning, parental controls, and limits on advertising to children. If a cable or satellite provider fails to satisfy these requirements, the Commission is able to ensure corrective measures by initiating an enforcement action.<sup>15</sup>

The NPRM seeks to ensure that these important and longstanding public interest features continue to be guaranteed in competitive set-top boxes and video apps that access cable and satellite content. We propose accomplishing this goal through a certification process, in which third-party devices' and apps' interoperability with cable and satellite networks will be conditioned on the devices' and apps' compliance with these public interest features.

The purpose of this certification is to ensure a clear set of rules and strong enforcement authority. We are seeking to adopt the best certification process, whether certification to consumers, certification to cable and satellite providers, certification to the Commission, or certification to an independent body to ensure compliance. The Federal Trade Commission, state attorneys general, and private litigants are generally able to pursue businesses that misrepresent their security and privacy practices. We anticipate that we and our partners at FTC would vigorously protect public interest features in competitive devices and apps, in much the same way that FCC already protects those same features in cable and satellite devices and apps. The NPRM seeks comment on these certification and enforcement mechanisms.

*3. How does the proposed rulemaking ensure that third-party device manufacturers and software developers are meeting an adequate level of software and hardware security, including supply chain risks?*

A business that offers a competitive set-top box or video app that accesses cable and satellite content would commit to adopting reasonable security safeguards. If a device manufacturer or software vendor failed to implement adequate precautions, it would risk enforcement action under the Federal Trade Commission Act and similar state statutes. Cable and satellite providers could also revoke interoperability with that set-top box or video app.

Under our proposal, a competitive device or app could also be subject to technical auditing for ensuring adequate content protection. The proposal would not alter the current landscape of DRM platforms, some of which require technical validation for a device or app to be

---

<sup>14</sup> *Id.* ¶ 73.

<sup>15</sup> *E.g.*, Cox Communications, Inc. Order and Consent Decree, 30 FCC Rcd. 12302 (Nov. 5, 2015) (enforcement action against a cable provider that did not adequately secure customer information).



compliant.<sup>16</sup> The NPRM seeks comment on whether independent testing should be required for other navigation device security properties.<sup>17</sup>

Responsibility for securing the internal networks of cable and satellite providers would remain with those providers. The FCC's proposal would not affect a cable or satellite provider's selection of products, services, integrators, suppliers, service providers, or other considerations for supply chain risk.

*4. Did the FCC consider the NIST Cybersecurity Framework risk management approach in the proposed rule-making?*

*a. If yes, please describe how and cite the references in the proposed rulemaking.*

Yes. FCC staff sought and received a broad range of security input, as discussed in response to Question #1. The NIST Cybersecurity Framework was one of many resources that Commission expert personnel consulted in the course of developing our proposal. FCC staff also considered recommendations from the Communications Security, Reliability, and Interoperability Council (CISRIC) IV Working Group 4, a technical advisory group charged with reporting NIST Cybersecurity Framework best practices for the communications sector.<sup>18</sup> DSTAC's final report cites NIST security guidance and technical standards.<sup>19</sup> The Commission has sought comment on both the DSTAC report and the set-top box proposal, and stakeholders have referenced the NIST Cybersecurity Framework.

*5. Does the proposed rulemaking address economic harm to content creators or businesses that may be impacted from the potential for cyberattacks or potential harm to infrastructure?*

In light of our comprehensive approach to security issues, our proposal does not increase the risk of economic harm to content creators or businesses as a result of cyberattacks. As addressed above and consistent with our duty under section 629(b) to protect system security, our proposal protects both the integrity of television delivery systems and the rights of content owners. Content creators will have the very same legal remedies available to them today to pursue individuals who pirate content<sup>20</sup> or circumvent copy protections.<sup>21</sup> Similarly, our proposal would not affect the legal remedies available to cable and satellite providers to pursue hackers.<sup>22</sup>

---

<sup>16</sup> Expanding Consumers' Video Navigation Choices, *supra* note 1, ¶ 71.

<sup>17</sup> *Id.* ¶¶ 72, 74.

<sup>18</sup> COMM'NS SEC., RELIABILITY & INTEROPERABILITY COUNCIL IV, CYBERSECURITY RISK MANAGEMENT AND BEST PRACTICES (Mar. 18, 2015),

[https://transition.fcc.gov/pshs/advisory/csr4/CSRIC\\_IV\\_WG4\\_Final\\_Report\\_031815.pdf](https://transition.fcc.gov/pshs/advisory/csr4/CSRIC_IV_WG4_Final_Report_031815.pdf).

<sup>19</sup> DSTAC FINAL REPORT, *supra* note 9, at 100, 186-92.

<sup>20</sup> *E.g.*, 47 U.S.C. §§ 501-506 (civil cause of action and criminal penalties for copyright infringement).

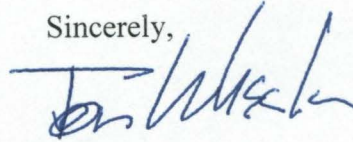
<sup>21</sup> *E.g.*, 17 U.S.C. § 1201 (civil cause of action and criminal penalties for circumventing content protections).

<sup>22</sup> *E.g.*, 18 U.S.C. § 1030 (civil cause of action and criminal penalties for computer trespass).



Thank you for your engagement on this important issue. As we develop a record and explore fulfilling our statutory mandate, I look forward to continuing to work with you on this important consumer issue.

Sincerely,

A handwritten signature in blue ink, appearing to read "Tom Wheeler", written over a horizontal line.

Tom Wheeler







FEDERAL COMMUNICATIONS COMMISSION  
WASHINGTON

OFFICE OF  
THE CHAIRMAN

June 10, 2016

The Honorable Ron Johnson  
Chairman  
Committee on Homeland Security and Governmental Affairs  
United States Senate  
340 Dirksen Senate Office Building  
Washington, D.C. 20510

Dear Chairman Johnson:

Thank you for your recent letter inquiring how the Federal Communications Commission (FCC) is addressing cybersecurity issues as part of our current rulemaking efforts to comply with the Communications Act's mandate for consumer choice in television navigation tools.

Protecting the nation's networks is a top priority for the FCC. Commission personnel work around the clock—including in a 24/7 operations center—to safeguard America's telephone, radio, cable, satellite, and Internet connectivity. The Commission takes our security responsibilities very seriously, and we leverage extensive staff expertise to ensure our policy proposals accord with best practices and the best available science.

We bring this cybersecurity experience and awareness to all of the rulemakings we undertake to fulfill our responsibilities under the Communications Act, including our current efforts to update our rules implementing section 629 of the Act. Adopted by Congress in 1996, section 629 requires the Commission to promote competition in the market for devices that consumers use to access their pay-television content.<sup>1</sup> The Notice of Proposed Rulemaking (NPRM) we adopted earlier this year proposes updating our rules implementing section 629 to allow device manufacturers and other innovators to develop devices or software that will give pay-television subscribers new ways to access the content they have purchased.<sup>2</sup>

We took this action because consumers have few alternatives to leasing set-top boxes from their pay-television providers. The statutory mandate is not yet filled. This lack of competition has meant few choices and high prices for consumers. In a recent Rasmussen Reports study, 84 percent of consumers felt their cable bill was too high. Included in every bill is a no-option, add-on fee for set top box rental. According to a congressional study, consumers spend, on average, \$231 in rental fees annually. Even worse for consumers, these rental fees continue to increase.<sup>3</sup> And while MVPD set-top boxes are increasingly connected to the Internet,

---

<sup>1</sup> 47 U.S.C. § 629.

<sup>2</sup> Expanding Consumers' Video Navigation Choices, 81 Fed. Reg. 14033 (proposed Mar. 16, 2016).

<sup>3</sup> One recent analysis found that the cost of cable set-top boxes has risen 185 percent since 1994 while the prices of computers, televisions, and mobile phones have dropped by 90 percent during that same time period. Consumer



they have been greatly outpaced in functionality and convenience by online video devices and apps.

The NPRM proposes a careful balance between network security and section 629's mandate that consumers be able to enjoy pay-television content with the equipment of their choice. Cable and satellite providers would be required to support a narrow, defined set of interfaces that would allow competitive devices and apps to access television content. These types of interfaces, usually termed Application Programming Interfaces (APIs), are routinely offered by online services. APIs allow a third party (such as a consumer navigation device provider) to interface with an organization's systems, without revealing any internal design, operation, or data about the organization. Third parties that connect to an API are not granted full system access, and are limited to only the features provided by the API. Securing an API is easier than securing internal systems, because an API only has to support specific functionality. Best practices for API security are readily available and widely practiced.<sup>4</sup>

The proposal would bring to television services the same secure modularity that phone and Internet customers have long enjoyed. In the telephone context, for example, a user can purchase and operate a third-party (e.g. Samsung) phone; the phone is not granted full access to telephone carrier (e.g. Verizon) internal systems. Similarly, in the Internet context, a user can purchase and operate a third-party (e.g. Arris) modem; that modem is not granted full access to the Internet Service Provider's (e.g. Comcast) internal systems.

All of the major cable and satellite providers, in fact, already support APIs for authenticating user credentials—some of the most sensitive information in the television ecosystem. Services like HBO Go<sup>5</sup> and Showtime Anytime<sup>6</sup> ensure that customers have subscribed by interfacing with cable and satellite account management systems. These APIs have been supported for over 5 years.

Finally, the FCC's set-top box proposal would in no way alter the role of digital rights management (DRM) platforms in the television ecosystem. DRM platforms offer rigorous protection against unauthorized copying and other violations of content owner rights.<sup>7</sup> Under the FCC's proposal, content owners would remain free to select the DRM platforms that they prefer. Developers of competitive set-top boxes and apps would license the DRM technology and satisfy compliance requirements – in the very same way that current set-top boxes support DRM, and the same way that competitive devices and apps already support DRM for online video.

---

Fed'n Am. & Pub. Knowledge, Comment Re: Media Bureau Request for Comment on DSTAC Report, MB Docket No. 15-64 (Jan. 20, 2016).

<sup>4</sup> See, e.g., *OWASP Enterprise Security API Project*, OPEN WEB APPLICATION SOC'Y PROJECT [https://www.owasp.org/index.php/Project\\_Information:\\_OWASP\\_Enterprise\\_Security\\_API\\_Project](https://www.owasp.org/index.php/Project_Information:_OWASP_Enterprise_Security_API_Project) (last visited June 2, 2016).

<sup>5</sup> HBO GO, <http://play.hbogo.com> (last visited June 2, 2016).

<sup>6</sup> SHOWTIME ANYTIME, <http://www.showtimeanytime.com> (last visited June 2, 2016).

<sup>7</sup> See DOWNLOADABLE SEC. TECH. ADVISORY COMM., DSTAC FINAL REPORT 262-67 (Aug. 28, 2015), <https://transition.fcc.gov/dstac/dstac-report-final-08282015.pdf> [hereinafter DSTAC FINAL REPORT].



Furthermore, all of the major DRM platforms support revoking authorization for content; if a competitive device or app were ever found to be violating DRM requirements, access to content could be immediately terminated.

Please find below answers to the specific questions in your letter.

*1. How did the FCC consider cybersecurity when developing the proposed rulemaking?*

The NPRM was prompted in part by a congressional directive within the STELA Reauthorization Act of 2014.<sup>8</sup> Section 106(d) of that legislation required FCC to assemble a working group of technical experts to evaluate and recommend options for enhancing downloadable security systems designed to promote the competitive availability of navigation devices. The FCC promptly implemented Congress's directive by chartering the Downloadable Security Technology Advisory Committee (DSTAC) on December 5, 2014.

This DSTAC's membership consisted of diverse technical experts, drawn from content creators, cable and satellite providers, consumer electronics manufacturers, software vendors, public interest organizations, and academia.<sup>9</sup> The group first convened on February 23, 2015. After weekly conference calls and additional in-person meetings, the committee issued its final 344-page report on August 28, 2015.<sup>10</sup> The FCC also received over 100 comments and other submissions in association with this process.<sup>11</sup> You can find this report and other DSTAC materials at: <https://www.fcc.gov/about-fcc/advisory-committees/general/downloadable-security-technology-advisory-committee>.

The DSTAC's participants and commenters provided valuable technical guidance to the Commission, with particular emphasis on security and privacy matters. Over 100 pages of the committee's final report expressly address cable and satellite network security, protecting content, or safeguarding consumer data.<sup>12</sup> Many comments and submissions also addressed security issues.

In sum, the FCC solicited and benefited from a wealth of security expertise while developing the proposed rulemaking, and we carefully evaluated the input that we received. The Notice of Proposed Rulemaking seeks additional input from stakeholders on the security aspects of the Commission's proposal.<sup>13</sup>

---

<sup>8</sup> STELA Reauthorization Act of 2014, Pub. L. No. 113-200, § 106(d), 128 Stat. 2059 (2014)

<sup>9</sup> *Appointment of Members to the Downloadable Security Technology Advisory Committee*, 30 FCC Rcd. 389 (Jan. 27, 2015).

<sup>10</sup> DSTAC FINAL REPORT, *supra* note 9.

<sup>11</sup> See MB Docket No. 15-64.

<sup>12</sup> See DSTAC FINAL REPORT, *supra* note 9, at 3-4, 12-16, 24-26, 28-30, 31-37, 47-56, 60-135, 186-192.

<sup>13</sup> Expanding Consumers' Video Navigation Choices, *supra* note 1, ¶¶ 50-62, 70-80.



*2. The FCC requires self-certifications related to a number of issues, how will the FCC enforce this?*

The Communications Act and Commission rules guarantee a set of public interest features for current cable and satellite set-top boxes.<sup>14</sup> These features include strong security and privacy protections, Emergency Alert System messaging, closed captioning, parental controls, and limits on advertising to children. If a cable or satellite provider fails to satisfy these requirements, the Commission is able to ensure corrective measures by initiating an enforcement action.<sup>15</sup>

The NPRM seeks to ensure that these important and longstanding public interest features continue to be guaranteed in competitive set-top boxes and video apps that access cable and satellite content. We propose accomplishing this goal through a certification process, in which third-party devices' and apps' interoperability with cable and satellite networks will be conditioned on the devices' and apps' compliance with these public interest features.

The purpose of this certification is to ensure a clear set of rules and strong enforcement authority. We are seeking to adopt the best certification process, whether certification to consumers, certification to cable and satellite providers, certification to the Commission, or certification to an independent body to ensure compliance. The Federal Trade Commission, state attorneys general, and private litigants are generally able to pursue businesses that misrepresent their security and privacy practices. We anticipate that we and our partners at FTC would vigorously protect public interest features in competitive devices and apps, in much the same way that FCC already protects those same features in cable and satellite devices and apps. The NPRM seeks comment on these certification and enforcement mechanisms.

*3. How does the proposed rulemaking ensure that third-party device manufacturers and software developers are meeting an adequate level of software and hardware security, including supply chain risks?*

A business that offers a competitive set-top box or video app that accesses cable and satellite content would commit to adopting reasonable security safeguards. If a device manufacturer or software vendor failed to implement adequate precautions, it would risk enforcement action under the Federal Trade Commission Act and similar state statutes. Cable and satellite providers could also revoke interoperability with that set-top box or video app.

Under our proposal, a competitive device or app could also be subject to technical auditing for ensuring adequate content protection. The proposal would not alter the current landscape of DRM platforms, some of which require technical validation for a device or app to be

---

<sup>14</sup> *Id.* ¶ 73.

<sup>15</sup> *E.g.*, Cox Communications, Inc. Order and Consent Decree, 30 FCC Rcd. 12302 (Nov. 5, 2015) (enforcement action against a cable provider that did not adequately secure customer information).



compliant.<sup>16</sup> The NPRM seeks comment on whether independent testing should be required for other navigation device security properties.<sup>17</sup>

Responsibility for securing the internal networks of cable and satellite providers would remain with those providers. The FCC's proposal would not affect a cable or satellite provider's selection of products, services, integrators, suppliers, service providers, or other considerations for supply chain risk.

*4. Did the FCC consider the NIST Cybersecurity Framework risk management approach in the proposed rule-making?*

*a. If yes, please describe how and cite the references in the proposed rulemaking.*

Yes. FCC staff sought and received a broad range of security input, as discussed in response to Question #1. The NIST Cybersecurity Framework was one of many resources that Commission expert personnel consulted in the course of developing our proposal. FCC staff also considered recommendations from the Communications Security, Reliability, and Interoperability Council (CISRIC) IV Working Group 4, a technical advisory group charged with reporting NIST Cybersecurity Framework best practices for the communications sector.<sup>18</sup> DSTAC's final report cites NIST security guidance and technical standards.<sup>19</sup> The Commission has sought comment on both the DSTAC report and the set-top box proposal, and stakeholders have referenced the NIST Cybersecurity Framework.

*5. Does the proposed rulemaking address economic harm to content creators or businesses that may be impacted from the potential for cyberattacks or potential harm to infrastructure?*

In light of our comprehensive approach to security issues, our proposal does not increase the risk of economic harm to content creators or businesses as a result of cyberattacks. As addressed above and consistent with our duty under section 629(b) to protect system security, our proposal protects both the integrity of television delivery systems and the rights of content owners. Content creators will have the very same legal remedies available to them today to pursue individuals who pirate content<sup>20</sup> or circumvent copy protections.<sup>21</sup> Similarly, our proposal would not affect the legal remedies available to cable and satellite providers to pursue hackers.<sup>22</sup>

---

<sup>16</sup> Expanding Consumers' Video Navigation Choices, *supra* note 1, ¶ 71.

<sup>17</sup> *Id.* ¶¶ 72, 74.

<sup>18</sup> COMM'NS SEC., RELIABILITY & INTEROPERABILITY COUNCIL IV, CYBERSECURITY RISK MANAGEMENT AND BEST PRACTICES (Mar. 18, 2015),

[https://transition.fcc.gov/pshs/advisory/csric4/CSRIC\\_IV\\_WG4\\_Final\\_Report\\_031815.pdf](https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf).

<sup>19</sup> DSTAC FINAL REPORT, *supra* note 9, at 100, 186-92.

<sup>20</sup> *E.g.*, 47 U.S.C. §§ 501-506 (civil cause of action and criminal penalties for copyright infringement).

<sup>21</sup> *E.g.*, 17 U.S.C. § 1201 (civil cause of action and criminal penalties for circumventing content protections).

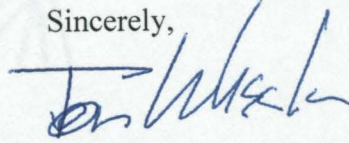
<sup>22</sup> *E.g.*, 18 U.S.C. § 1030 (civil cause of action and criminal penalties for computer trespass).



Page 6—The Honorable Ron Johnson

Thank you for your engagement on this important issue. As we develop a record and explore fulfilling our statutory mandate, I look forward to continuing to work with you on this important consumer issue.

Sincerely,

A handwritten signature in blue ink, appearing to read "Tom Wheeler", written over a faint circular seal and the year "2013".

Tom Wheeler





FEDERAL COMMUNICATIONS COMMISSION  
WASHINGTON

OFFICE OF  
THE CHAIRMAN

June 10, 2016

The Honorable Michael McCaul  
Chairman  
Committee on Homeland Security  
U.S. House of Representatives  
H2-176 Ford House Office Building  
Washington, D.C. 20515

Dear Chairman McCaul:

Thank you for your recent letter inquiring how the Federal Communications Commission (FCC) is addressing cybersecurity issues as part of our current rulemaking efforts to comply with the Communications Act's mandate for consumer choice in television navigation tools.

Protecting the nation's networks is a top priority for the FCC. Commission personnel work around the clock—including in a 24/7 operations center—to safeguard America's telephone, radio, cable, satellite, and Internet connectivity. The Commission takes our security responsibilities very seriously, and we leverage extensive staff expertise to ensure our policy proposals accord with best practices and the best available science.

We bring this cybersecurity experience and awareness to all of the rulemakings we undertake to fulfill our responsibilities under the Communications Act, including our current efforts to update our rules implementing section 629 of the Act. Adopted by Congress in 1996, section 629 requires the Commission to promote competition in the market for devices that consumers use to access their pay-television content.<sup>1</sup> The Notice of Proposed Rulemaking (NPRM) we adopted earlier this year proposes updating our rules implementing section 629 to allow device manufacturers and other innovators to develop devices or software that will give pay-television subscribers new ways to access the content they have purchased.<sup>2</sup>

We took this action because consumers have few alternatives to leasing set-top boxes from their pay-television providers. The statutory mandate is not yet filled. This lack of competition has meant few choices and high prices for consumers. In a recent Rasmussen Reports study, 84 percent of consumers felt their cable bill was too high. Included in every bill is a no-option, add-on fee for set top box rental. According to a congressional study, consumers spend, on average, \$231 in rental fees annually. Even worse for consumers, these rental fees continue to increase.<sup>3</sup> And while MVPD set-top boxes are increasingly connected to the Internet,

---

<sup>1</sup> 47 U.S.C. § 629.

<sup>2</sup> Expanding Consumers' Video Navigation Choices, 81 Fed. Reg. 14033 (proposed Mar. 16, 2016).

<sup>3</sup> One recent analysis found that the cost of cable set-top boxes has risen 185 percent since 1994 while the prices of computers, televisions, and mobile phones have dropped by 90 percent during that same time period. Consumer



they have been greatly outpaced in functionality and convenience by online video devices and apps.

The NPRM proposes a careful balance between network security and section 629's mandate that consumers be able to enjoy pay-television content with the equipment of their choice. Cable and satellite providers would be required to support a narrow, defined set of interfaces that would allow competitive devices and apps to access television content. These types of interfaces, usually termed Application Programming Interfaces (APIs), are routinely offered by online services. APIs allow a third party (such as a consumer navigation device provider) to interface with an organization's systems, without revealing any internal design, operation, or data about the organization. Third parties that connect to an API are not granted full system access, and are limited to only the features provided by the API. Securing an API is easier than securing internal systems, because an API only has to support specific functionality. Best practices for API security are readily available and widely practiced.<sup>4</sup>

The proposal would bring to television services the same secure modularity that phone and Internet customers have long enjoyed. In the telephone context, for example, a user can purchase and operate a third-party (e.g. Samsung) phone; the phone is not granted full access to telephone carrier (e.g. Verizon) internal systems. Similarly, in the Internet context, a user can purchase and operate a third-party (e.g. Arris) modem; that modem is not granted full access to the Internet Service Provider's (e.g. Comcast) internal systems.

All of the major cable and satellite providers, in fact, already support APIs for authenticating user credentials—some of the most sensitive information in the television ecosystem. Services like HBO Go<sup>5</sup> and Showtime Anytime<sup>6</sup> ensure that customers have subscribed by interfacing with cable and satellite account management systems. These APIs have been supported for over 5 years.

Finally, the FCC's set-top box proposal would in no way alter the role of digital rights management (DRM) platforms in the television ecosystem. DRM platforms offer rigorous protection against unauthorized copying and other violations of content owner rights.<sup>7</sup> Under the FCC's proposal, content owners would remain free to select the DRM platforms that they prefer. Developers of competitive set-top boxes and apps would license the DRM technology and satisfy compliance requirements – in the very same way that current set-top boxes support DRM, and the same way that competitive devices and apps already support DRM for online video.

---

Fed'n Am. & Pub. Knowledge, Comment Re: Media Bureau Request for Comment on DSTAC Report, MB Docket No. 15-64 (Jan. 20, 2016).

<sup>4</sup> See, e.g., *OWASP Enterprise Security API Project*, OPEN WEB APPLICATION SOC'Y PROJECT [https://www.owasp.org/index.php/Project\\_Information:\\_OWASP\\_Enterprise\\_Security\\_API\\_Project](https://www.owasp.org/index.php/Project_Information:_OWASP_Enterprise_Security_API_Project) (last visited June 2, 2016).

<sup>5</sup> HBO GO, <http://play.hbogo.com> (last visited June 2, 2016).

<sup>6</sup> SHOWTIME ANYTIME, <http://www.showtimeanytime.com> (last visited June 2, 2016).

<sup>7</sup> See DOWNLOADABLE SEC. TECH. ADVISORY COMM., DSTAC FINAL REPORT 262-67 (Aug. 28, 2015), <https://transition.fcc.gov/dstac/dstac-report-final-08282015.pdf> [hereinafter DSTAC FINAL REPORT].



Furthermore, all of the major DRM platforms support revoking authorization for content; if a competitive device or app were ever found to be violating DRM requirements, access to content could be immediately terminated.

Please find below answers to the specific questions in your letter.

*1. How did the FCC consider cybersecurity when developing the proposed rulemaking?*

The NPRM was prompted in part by a congressional directive within the STELA Reauthorization Act of 2014.<sup>8</sup> Section 106(d) of that legislation required FCC to assemble a working group of technical experts to evaluate and recommend options for enhancing downloadable security systems designed to promote the competitive availability of navigation devices. The FCC promptly implemented Congress's directive by chartering the Downloadable Security Technology Advisory Committee (DSTAC) on December 5, 2014.

This DSTAC's membership consisted of diverse technical experts, drawn from content creators, cable and satellite providers, consumer electronics manufacturers, software vendors, public interest organizations, and academia.<sup>9</sup> The group first convened on February 23, 2015. After weekly conference calls and additional in-person meetings, the committee issued its final 344-page report on August 28, 2015.<sup>10</sup> The FCC also received over 100 comments and other submissions in association with this process.<sup>11</sup> You can find this report and other DSTAC materials at: <https://www.fcc.gov/about-fcc/advisory-committees/general/downloadable-security-technology-advisory-committee>.

The DSTAC's participants and commenters provided valuable technical guidance to the Commission, with particular emphasis on security and privacy matters. Over 100 pages of the committee's final report expressly address cable and satellite network security, protecting content, or safeguarding consumer data.<sup>12</sup> Many comments and submissions also addressed security issues.

In sum, the FCC solicited and benefited from a wealth of security expertise while developing the proposed rulemaking, and we carefully evaluated the input that we received. The Notice of Proposed Rulemaking seeks additional input from stakeholders on the security aspects of the Commission's proposal.<sup>13</sup>

---

<sup>8</sup> STELA Reauthorization Act of 2014, Pub. L. No. 113-200, § 106(d), 128 Stat. 2059 (2014)

<sup>9</sup> *Appointment of Members to the Downloadable Security Technology Advisory Committee*, 30 FCC Rcd. 389 (Jan. 27, 2015).

<sup>10</sup> DSTAC FINAL REPORT, *supra* note 9.

<sup>11</sup> See MB Docket No. 15-64.

<sup>12</sup> See DSTAC FINAL REPORT, *supra* note 9, at 3-4, 12-16, 24-26, 28-30, 31-37, 47-56, 60-135, 186-192.

<sup>13</sup> Expanding Consumers' Video Navigation Choices, *supra* note 1, ¶¶ 50-62, 70-80.



*2. The FCC requires self-certifications related to a number of issues, how will the FCC enforce this?*

The Communications Act and Commission rules guarantee a set of public interest features for current cable and satellite set-top boxes.<sup>14</sup> These features include strong security and privacy protections, Emergency Alert System messaging, closed captioning, parental controls, and limits on advertising to children. If a cable or satellite provider fails to satisfy these requirements, the Commission is able to ensure corrective measures by initiating an enforcement action.<sup>15</sup>

The NPRM seeks to ensure that these important and longstanding public interest features continue to be guaranteed in competitive set-top boxes and video apps that access cable and satellite content. We propose accomplishing this goal through a certification process, in which third-party devices' and apps' interoperability with cable and satellite networks will be conditioned on the devices' and apps' compliance with these public interest features.

The purpose of this certification is to ensure a clear set of rules and strong enforcement authority. We are seeking to adopt the best certification process, whether certification to consumers, certification to cable and satellite providers, certification to the Commission, or certification to an independent body to ensure compliance. The Federal Trade Commission, state attorneys general, and private litigants are generally able to pursue businesses that misrepresent their security and privacy practices. We anticipate that we and our partners at FTC would vigorously protect public interest features in competitive devices and apps, in much the same way that FCC already protects those same features in cable and satellite devices and apps. The NPRM seeks comment on these certification and enforcement mechanisms.

*3. How does the proposed rulemaking ensure that third-party device manufacturers and software developers are meeting an adequate level of software and hardware security, including supply chain risks?*

A business that offers a competitive set-top box or video app that accesses cable and satellite content would commit to adopting reasonable security safeguards. If a device manufacturer or software vendor failed to implement adequate precautions, it would risk enforcement action under the Federal Trade Commission Act and similar state statutes. Cable and satellite providers could also revoke interoperability with that set-top box or video app.

Under our proposal, a competitive device or app could also be subject to technical auditing for ensuring adequate content protection. The proposal would not alter the current landscape of DRM platforms, some of which require technical validation for a device or app to be

---

<sup>14</sup> *Id.* ¶ 73.

<sup>15</sup> *E.g.*, Cox Communications, Inc. Order and Consent Decree, 30 FCC Rcd. 12302 (Nov. 5, 2015) (enforcement action against a cable provider that did not adequately secure customer information).



compliant.<sup>16</sup> The NPRM seeks comment on whether independent testing should be required for other navigation device security properties.<sup>17</sup>

Responsibility for securing the internal networks of cable and satellite providers would remain with those providers. The FCC's proposal would not affect a cable or satellite provider's selection of products, services, integrators, suppliers, service providers, or other considerations for supply chain risk.

*4. Did the FCC consider the NIST Cybersecurity Framework risk management approach in the proposed rule-making?*

*a. If yes, please describe how and cite the references in the proposed rulemaking.*

Yes. FCC staff sought and received a broad range of security input, as discussed in response to Question #1. The NIST Cybersecurity Framework was one of many resources that Commission expert personnel consulted in the course of developing our proposal. FCC staff also considered recommendations from the Communications Security, Reliability, and Interoperability Council (CISRIC) IV Working Group 4, a technical advisory group charged with reporting NIST Cybersecurity Framework best practices for the communications sector.<sup>18</sup> DSTAC's final report cites NIST security guidance and technical standards.<sup>19</sup> The Commission has sought comment on both the DSTAC report and the set-top box proposal, and stakeholders have referenced the NIST Cybersecurity Framework.

*5. Does the proposed rulemaking address economic harm to content creators or businesses that may be impacted from the potential for cyberattacks or potential harm to infrastructure?*

In light of our comprehensive approach to security issues, our proposal does not increase the risk of economic harm to content creators or businesses as a result of cyberattacks. As addressed above and consistent with our duty under section 629(b) to protect system security, our proposal protects both the integrity of television delivery systems and the rights of content owners. Content creators will have the very same legal remedies available to them today to pursue individuals who pirate content<sup>20</sup> or circumvent copy protections.<sup>21</sup> Similarly, our proposal would not affect the legal remedies available to cable and satellite providers to pursue hackers.<sup>22</sup>

---

<sup>16</sup> Expanding Consumers' Video Navigation Choices, *supra* note 1, ¶ 71.

<sup>17</sup> *Id.* ¶¶ 72, 74.

<sup>18</sup> COMM'NS SEC., RELIABILITY & INTEROPERABILITY COUNCIL IV, CYBERSECURITY RISK MANAGEMENT AND BEST PRACTICES (Mar. 18, 2015),

[https://transition.fcc.gov/pshs/advisory/csric4/CSRIC\\_IV\\_WG4\\_Final\\_Report\\_031815.pdf](https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf).

<sup>19</sup> DSTAC FINAL REPORT, *supra* note 9, at 100, 186-92.

<sup>20</sup> *E.g.*, 47 U.S.C. §§ 501-506 (civil cause of action and criminal penalties for copyright infringement).

<sup>21</sup> *E.g.*, 17 U.S.C. § 1201 (civil cause of action and criminal penalties for circumventing content protections).

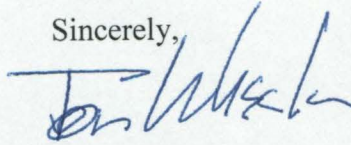
<sup>22</sup> *E.g.*, 18 U.S.C. § 1030 (civil cause of action and criminal penalties for computer trespass).



Page 6—The Honorable Michael McCaul

Thank you for your engagement on this important issue. As we develop a record and explore fulfilling our statutory mandate, I look forward to continuing to work with you on this important consumer issue.

Sincerely,

A handwritten signature in blue ink, appearing to read "Tom Wheeler", with a stylized, flowing script.

Tom Wheeler







FEDERAL COMMUNICATIONS COMMISSION  
WASHINGTON

OFFICE OF  
THE CHAIRMAN

June 10, 2016

The Honorable Bennie Thompson  
Ranking Member  
Committee on Homeland Security  
U.S. House of Representatives  
H2-117 Ford House Office Building  
Washington, D.C. 20515

Dear Congressman Thompson:

Thank you for your recent letter inquiring how the Federal Communications Commission (FCC) is addressing cybersecurity issues as part of our current rulemaking efforts to comply with the Communications Act's mandate for consumer choice in television navigation tools.

Protecting the nation's networks is a top priority for the FCC. Commission personnel work around the clock—including in a 24/7 operations center—to safeguard America's telephone, radio, cable, satellite, and Internet connectivity. The Commission takes our security responsibilities very seriously, and we leverage extensive staff expertise to ensure our policy proposals accord with best practices and the best available science.

We bring this cybersecurity experience and awareness to all of the rulemakings we undertake to fulfill our responsibilities under the Communications Act, including our current efforts to update our rules implementing section 629 of the Act. Adopted by Congress in 1996, section 629 requires the Commission to promote competition in the market for devices that consumers use to access their pay-television content.<sup>1</sup> The Notice of Proposed Rulemaking (NPRM) we adopted earlier this year proposes updating our rules implementing section 629 to allow device manufacturers and other innovators to develop devices or software that will give pay-television subscribers new ways to access the content they have purchased.<sup>2</sup>

We took this action because consumers have few alternatives to leasing set-top boxes from their pay-television providers. The statutory mandate is not yet filled. This lack of competition has meant few choices and high prices for consumers. In a recent Rasmussen Reports study, 84 percent of consumers felt their cable bill was too high. Included in every bill is a no-option, add-on fee for set top box rental. According to a congressional study, consumers spend, on average, \$231 in rental fees annually. Even worse for consumers, these rental fees continue to increase.<sup>3</sup> And while MVPD set-top boxes are increasingly connected to the Internet,

---

<sup>1</sup> 47 U.S.C. § 629.

<sup>2</sup> Expanding Consumers' Video Navigation Choices, 81 Fed. Reg. 14033 (proposed Mar. 16, 2016).

<sup>3</sup> One recent analysis found that the cost of cable set-top boxes has risen 185 percent since 1994 while the prices of computers, televisions, and mobile phones have dropped by 90 percent during that same time period. Consumer



they have been greatly outpaced in functionality and convenience by online video devices and apps.

The NPRM proposes a careful balance between network security and section 629's mandate that consumers be able to enjoy pay-television content with the equipment of their choice. Cable and satellite providers would be required to support a narrow, defined set of interfaces that would allow competitive devices and apps to access television content. These types of interfaces, usually termed Application Programming Interfaces (APIs), are routinely offered by online services. APIs allow a third party (such as a consumer navigation device provider) to interface with an organization's systems, without revealing any internal design, operation, or data about the organization. Third parties that connect to an API are not granted full system access, and are limited to only the features provided by the API. Securing an API is easier than securing internal systems, because an API only has to support specific functionality. Best practices for API security are readily available and widely practiced.<sup>4</sup>

The proposal would bring to television services the same secure modularity that phone and Internet customers have long enjoyed. In the telephone context, for example, a user can purchase and operate a third-party (e.g. Samsung) phone; the phone is not granted full access to telephone carrier (e.g. Verizon) internal systems. Similarly, in the Internet context, a user can purchase and operate a third-party (e.g. Arris) modem; that modem is not granted full access to the Internet Service Provider's (e.g. Comcast) internal systems.

All of the major cable and satellite providers, in fact, already support APIs for authenticating user credentials—some of the most sensitive information in the television ecosystem. Services like HBO Go<sup>5</sup> and Showtime Anytime<sup>6</sup> ensure that customers have subscribed by interfacing with cable and satellite account management systems. These APIs have been supported for over 5 years.

Finally, the FCC's set-top box proposal would in no way alter the role of digital rights management (DRM) platforms in the television ecosystem. DRM platforms offer rigorous protection against unauthorized copying and other violations of content owner rights.<sup>7</sup> Under the FCC's proposal, content owners would remain free to select the DRM platforms that they prefer. Developers of competitive set-top boxes and apps would license the DRM technology and satisfy compliance requirements – in the very same way that current set-top boxes support DRM, and the same way that competitive devices and apps already support DRM for online video.

---

Fed'n Am. & Pub. Knowledge, Comment Re: Media Bureau Request for Comment on DSTAC Report, MB Docket No. 15-64 (Jan. 20, 2016).

<sup>4</sup> See, e.g., *OWASP Enterprise Security API Project*, OPEN WEB APPLICATION SOC'Y PROJECT [https://www.owasp.org/index.php/Project\\_Information:\\_OWASP\\_Enterprise\\_Security\\_API\\_Project](https://www.owasp.org/index.php/Project_Information:_OWASP_Enterprise_Security_API_Project) (last visited June 2, 2016).

<sup>5</sup> HBO GO, <http://play.hbogo.com> (last visited June 2, 2016).

<sup>6</sup> SHOWTIME ANYTIME, <http://www.showtimeanytime.com> (last visited June 2, 2016).

<sup>7</sup> See DOWNLOADABLE SEC. TECH. ADVISORY COMM., DSTAC FINAL REPORT 262-67 (Aug. 28, 2015), <https://transition.fcc.gov/dstac/dstac-report-final-08282015.pdf> [hereinafter DSTAC FINAL REPORT].



Furthermore, all of the major DRM platforms support revoking authorization for content; if a competitive device or app were ever found to be violating DRM requirements, access to content could be immediately terminated.

Please find below answers to the specific questions in your letter.

*1. How did the FCC consider cybersecurity when developing the proposed rulemaking?*

The NPRM was prompted in part by a congressional directive within the STELA Reauthorization Act of 2014.<sup>8</sup> Section 106(d) of that legislation required FCC to assemble a working group of technical experts to evaluate and recommend options for enhancing downloadable security systems designed to promote the competitive availability of navigation devices. The FCC promptly implemented Congress's directive by chartering the Downloadable Security Technology Advisory Committee (DSTAC) on December 5, 2014.

This DSTAC's membership consisted of diverse technical experts, drawn from content creators, cable and satellite providers, consumer electronics manufacturers, software vendors, public interest organizations, and academia.<sup>9</sup> The group first convened on February 23, 2015. After weekly conference calls and additional in-person meetings, the committee issued its final 344-page report on August 28, 2015.<sup>10</sup> The FCC also received over 100 comments and other submissions in association with this process.<sup>11</sup> You can find this report and other DSTAC materials at: <https://www.fcc.gov/about-fcc/advisory-committees/general/downloadable-security-technology-advisory-committee>.

The DSTAC's participants and commenters provided valuable technical guidance to the Commission, with particular emphasis on security and privacy matters. Over 100 pages of the committee's final report expressly address cable and satellite network security, protecting content, or safeguarding consumer data.<sup>12</sup> Many comments and submissions also addressed security issues.

In sum, the FCC solicited and benefited from a wealth of security expertise while developing the proposed rulemaking, and we carefully evaluated the input that we received. The Notice of Proposed Rulemaking seeks additional input from stakeholders on the security aspects of the Commission's proposal.<sup>13</sup>

---

<sup>8</sup> STELA Reauthorization Act of 2014, Pub. L. No. 113-200, § 106(d), 128 Stat. 2059 (2014)

<sup>9</sup> *Appointment of Members to the Downloadable Security Technology Advisory Committee*, 30 FCC Rcd. 389 (Jan. 27, 2015).

<sup>10</sup> DSTAC FINAL REPORT, *supra* note 9.

<sup>11</sup> See MB Docket No. 15-64.

<sup>12</sup> See DSTAC FINAL REPORT, *supra* note 9, at 3-4, 12-16, 24-26, 28-30, 31-37, 47-56, 60-135, 186-192.

<sup>13</sup> Expanding Consumers' Video Navigation Choices, *supra* note 1, ¶¶ 50-62, 70-80.



*2. The FCC requires self-certifications related to a number of issues, how will the FCC enforce this?*

The Communications Act and Commission rules guarantee a set of public interest features for current cable and satellite set-top boxes.<sup>14</sup> These features include strong security and privacy protections, Emergency Alert System messaging, closed captioning, parental controls, and limits on advertising to children. If a cable or satellite provider fails to satisfy these requirements, the Commission is able to ensure corrective measures by initiating an enforcement action.<sup>15</sup>

The NPRM seeks to ensure that these important and longstanding public interest features continue to be guaranteed in competitive set-top boxes and video apps that access cable and satellite content. We propose accomplishing this goal through a certification process, in which third-party devices' and apps' interoperability with cable and satellite networks will be conditioned on the devices' and apps' compliance with these public interest features.

The purpose of this certification is to ensure a clear set of rules and strong enforcement authority. We are seeking to adopt the best certification process, whether certification to consumers, certification to cable and satellite providers, certification to the Commission, or certification to an independent body to ensure compliance. The Federal Trade Commission, state attorneys general, and private litigants are generally able to pursue businesses that misrepresent their security and privacy practices. We anticipate that we and our partners at FTC would vigorously protect public interest features in competitive devices and apps, in much the same way that FCC already protects those same features in cable and satellite devices and apps. The NPRM seeks comment on these certification and enforcement mechanisms.

*3. How does the proposed rulemaking ensure that third-party device manufacturers and software developers are meeting an adequate level of software and hardware security, including supply chain risks?*

A business that offers a competitive set-top box or video app that accesses cable and satellite content would commit to adopting reasonable security safeguards. If a device manufacturer or software vendor failed to implement adequate precautions, it would risk enforcement action under the Federal Trade Commission Act and similar state statutes. Cable and satellite providers could also revoke interoperability with that set-top box or video app.

Under our proposal, a competitive device or app could also be subject to technical auditing for ensuring adequate content protection. The proposal would not alter the current landscape of DRM platforms, some of which require technical validation for a device or app to be

---

<sup>14</sup> *Id.* ¶ 73.

<sup>15</sup> *E.g.*, Cox Communications, Inc. Order and Consent Decree, 30 FCC Rcd. 12302 (Nov. 5, 2015) (enforcement action against a cable provider that did not adequately secure customer information).



compliant.<sup>16</sup> The NPRM seeks comment on whether independent testing should be required for other navigation device security properties.<sup>17</sup>

Responsibility for securing the internal networks of cable and satellite providers would remain with those providers. The FCC's proposal would not affect a cable or satellite provider's selection of products, services, integrators, suppliers, service providers, or other considerations for supply chain risk.

*4. Did the FCC consider the NIST Cybersecurity Framework risk management approach in the proposed rule-making?*

*a. If yes, please describe how and cite the references in the proposed rulemaking.*

Yes. FCC staff sought and received a broad range of security input, as discussed in response to Question #1. The NIST Cybersecurity Framework was one of many resources that Commission expert personnel consulted in the course of developing our proposal. FCC staff also considered recommendations from the Communications Security, Reliability, and Interoperability Council (CISRIC) IV Working Group 4, a technical advisory group charged with reporting NIST Cybersecurity Framework best practices for the communications sector.<sup>18</sup> DSTAC's final report cites NIST security guidance and technical standards.<sup>19</sup> The Commission has sought comment on both the DSTAC report and the set-top box proposal, and stakeholders have referenced the NIST Cybersecurity Framework.

*5. Does the proposed rulemaking address economic harm to content creators or businesses that may be impacted from the potential for cyberattacks or potential harm to infrastructure?*

In light of our comprehensive approach to security issues, our proposal does not increase the risk of economic harm to content creators or businesses as a result of cyberattacks. As addressed above and consistent with our duty under section 629(b) to protect system security, our proposal protects both the integrity of television delivery systems and the rights of content owners. Content creators will have the very same legal remedies available to them today to pursue individuals who pirate content<sup>20</sup> or circumvent copy protections.<sup>21</sup> Similarly, our proposal would not affect the legal remedies available to cable and satellite providers to pursue hackers.<sup>22</sup>

---

<sup>16</sup> Expanding Consumers' Video Navigation Choices, *supra* note 1, ¶ 71.

<sup>17</sup> *Id.* ¶¶ 72, 74.

<sup>18</sup> COMM'NS SEC., RELIABILITY & INTEROPERABILITY COUNCIL IV, CYBERSECURITY RISK MANAGEMENT AND BEST PRACTICES (Mar. 18, 2015),

[https://transition.fcc.gov/pshs/advisory/csric4/CSRIC\\_IV\\_WG4\\_Final\\_Report\\_031815.pdf](https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf).

<sup>19</sup> DSTAC FINAL REPORT, *supra* note 9, at 100, 186-92.

<sup>20</sup> *E.g.*, 47 U.S.C. §§ 501-506 (civil cause of action and criminal penalties for copyright infringement).

<sup>21</sup> *E.g.*, 17 U.S.C. § 1201 (civil cause of action and criminal penalties for circumventing content protections).

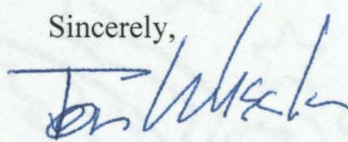
<sup>22</sup> *E.g.*, 18 U.S.C. § 1030 (civil cause of action and criminal penalties for computer trespass).



Page 6—The Honorable Bennie Thompson

Thank you for your engagement on this important issue. As we develop a record and explore fulfilling our statutory mandate, I look forward to continuing to work with you on this important consumer issue.

Sincerely,

A handwritten signature in blue ink, appearing to read "Tom Wheeler", written over a faint background watermark of the U.S. Department of Justice seal.

Tom Wheeler